REMARKS

In the Office Action of July 6, 2007, claims 3 and 4 were rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent 6,453,345 to Trcka et al. Claims 3, 4, 6, 7 and 9 were rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent 6,279,113 to Vaidya et al. Claims 5 and 8 were rejected under 35 U.S.C. 103(a) as unpatentable over Vaidya in view of Patent Application Publication 2003/0188189 to Desai et al. Claim 10 was rejected under 35 U.S.C. 103(a) as unpatentable over Vaidya in view of U.S. Patent 7,120,931 to Cheriton and U.S. Patent 6,424,654 to Daizo. And claims 11 and 12 were rejected under 35 U.S.C. 103(a) as unpatentable over Vaidya, Cheriton and Daizo in view of Desai. Claim 3 was also rejected under 35 U.S.C. 101 as directed to non-statutory subject matter.

Minor changes have been made in the specification to correct errors that arose during its preparation. No new matter has been added.

Paragraph 0004 has been amended as requested to insert the patent number for the referenced application. Paragraph 0011 has also been amended as requested to insert the application number and filing date as well as the patent number for the referenced provisional application. Applicants are still seeking the application number and filing date for the provisional application referenced in paragraph 0010.

Numerous changes were required in the claims because of informalities and indefiniteness. The claims have been revised extensively and these requirements have been addressed.

Changes were also required in Figs. 8 and 9 of the drawings. These changes have been made.

Applicants' invention is a method and apparatus for detecting malicious activity on a communication network. This activity includes attacks such as those that are intended to secure proprietary information or interfere with the operation of a computer as well as probes and scans which typically precede an attack. As set forth in paragraph 0017 of applicants' specification, a probe is an attempt to connect with a targeted network device. A scan is a systematic group of probes originating from a single source computer or group of computers.

Prior art attack detection methods include misuse detection and anomaly detection. Misuse detection compares on-line activity with signatures of known malicious behavior. While requiring relatively low computational resources, misuse detection requires that the attack signatures be known in advance and therefore cannot detect new types of attack. Anomaly detection evaluates network activity with respect to a model of normal behavior and identifies inconsistent behavior as anomalous. Since not all anomalous behavior is malicious, problems arise in maximizing the detection of malicious behavior while minimizing the rate of false alarms. In general, anomaly detection systems are computationally expensive.

As its title indicates, the primary reference Vaidya is directed to a signature-based attack detection system. The primary reference Trcka is directed to a network security and surveillance system. Neither reference mentions probes or scans.

More particularly, Trcka describes a system that records traffic on a communication network and then analyzes it in a variety of ways. These analysis functions are described at Col. 19, line 45 to Col. 22, line 58 and are listed in box 200 of FIG. 12. These functions include audit, problem determination, lost data recovery,

security violations, network operating characteristics, damage assessment/recovery, network problem solving, special non-network event and data replay. The audit application is described in more detail in FIGS. 12-15 and at Col. 22, line 60 to Col. 23, line 46. The problem determination function is described in more detail in FIGS. 16-19 and at Col. 23, lines 47-61. In general, the user is allowed to select for display a variety of predetermined events that occur within a specified time frame. Of particular interest, the user is able to list all logons by time, address and user ID as shown in FIG. 15 and can similarly list all failed logons as shown in FIG. 19. However, the is no disclosure of any further processing of the logons or failed logons.

Thus, Trcka fails to disclose applicants' method of detecting surveillance probes as recited in claim 3. To emphasize the differences between applicants' claim 3 and Trcka, claim 3 has been amended to explicitly recite a method for detecting surveillance probes, to recite the step of processing messages from the communication network to form connection sessions by clustering certain types of packets and to recite the step of detecting a surveillance probe by grouping connection sessions into groups, scoring the groups and generating an alert for groups whose score exceeds a threshold.

It is respectfully submitted that Trcka does not disclose the grouping of connection sessions, the scoring of the groups or the generation of an alert. Trcka's zoom in feature referred to by the Examiner merely allows the user "to view specific packet or transaction details." (Trcka, Col. 18, line 46).

It is also respectfully submitted that claim 3 as amended meets the requirements of 35 U.S.C. 101 in reciting a concrete and tangible result, the generation of an alarm.

Claim 3 as amended is also believed to be patentable over Vaidya. As emphasized above, Vaidya is a signature based attack detection system. Vaidya detects attacks by comparing activity on the communication network with signature profiles stored in the system. As noted by Vaidya at Col. 7, lines 46-48, the signature profiles may be a single expression such as the identity of a source address or a series of expressions. However, the signatures are predetermined.

To emphasize the differences between applicants' claim 3 and Vaidya, claim 3 has been amended to recite that the packets that are clustered are a) exchanged between addresses that are not predetermined; or b) have certain flags set; or c) have addresses that are not predetermined but have similar characteristics.

Since Vaidya does not disclose any non-signature method, it is respectfully submitted that Vaidya does not disclose claim 3 as amended.

Dependent claims 5-12 and newly added dependent claims 19-21 are believed patentable for the same reason claim 3 is patentable.

If the Examiner believes a telephone interview would expedite prosecution of this application, he is invited to call applicants' attorney at the number given below.

Aside for the fee for an extension of time, no additional fee is believed due for filing this response. However, if a fee is due, please charge such fee to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310.

Respectfully submitted,

55,302

Date: January 7, 2007

Francis E. Morris
Reg. No. 24,615
MORGAN, LEWIS & BOCKIUS LLP
Customer No. 009629
(212) 309-6632